UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

GARY MCNAIR,

Plaintiff,

v.

BATTELLE MEMORIAL INSTITUTE, dba PACIFIC NORTHWEST NATIONAL LABORATORY,

Defendant.

NO. CV-10-5147-RHW

PROTECTIVE ORDER

Pursuant to the parties' Stipulation, the Court enters the following Protective Order:

Sensitive Security Information: 49 U.S.C. § 114(r) and 49 C.F.R. Part 1520

1. Sensitive Security Information ("SSI") is a specific category of information that requires protection against unauthorized disclosure pursuant to 49 U.S.C. § 114(r) and 49 C.F.R. Part 1520. Unauthorized disclosure of SSI may be detrimental to the security of transportation, may constitute an unwarranted invasion of personal privacy, or may reveal a trade secret or privileged or confidential commercial or financial information. Unauthorized disclosure may also result in a civil enforcement penalty or other enforcement action by the Transportation Security Administration ("TSA") against the party making the unauthorized disclosure. 49 C.F.R. § 1520.17.

2. Access is limited to "covered persons" with a "need to know" as set forth in 49 C.F.R. § 1520.7 and § 1520.11. Because the parties, their attorneys, the Court and its employees are "covered persons" "with a need to know" the SSI

relevant to this case, this order permits the sharing through discovery in this civil action of relevant information and materials that are marked as SSI or that may otherwise contain SSI provided that Plaintiff had access to such information during his employment with Battelle Memorial Institute. The right of access to discovery materials marked as SSI or that may contain SSI shall be limited to the Court and its employees, Plaintiff, and counsel for the parties, paralegal, secretarial and clerical personnel in their employ. Court reporters retained by the parties for purposes recording depositions and who have signed a DHS-approved Non-Disclosure Agreement may also have access to SSI.

3. "Covered persons" have an express duty to protect against the unauthorized disclosure of SSI. 49 C.F.R. § 1520.9. SSI must be safeguarded in such a way that it is not physically or visually accessible to persons who do not have a "need to know," as defined in 49 C.F.R. § 1520.11. When unattended, SSI must be secured in a locked container or office, or other restricted access area.

4. Documents that contain SSI may not be further disseminated to persons without a "need to know" except with written permission from TSA. SSI must not be disclosed by either party to any person or entity other than those enumerated in paragraph two.

5. Documents that are marked SSI, or though not marked, contain SSI shall be treated as confidential and shall not be published or made available to the general public in any form (whether in paper or electronic form), but instead shall be filed under seal. In order to avoid the inadvertent unsealed filing, the parties shall to take all efforts to avoid the unnecessary filing of SSI with the Court.

6. The parties and their representatives are responsible for compliance with the training, physical protection and non-disclosure requirements described in 49 CFR 1520. For the convenience of the Court and the parties a TSA quick reference guide of the regulation is attached as Exhibit 1. However, the ultimate authority governing the protection of SSI is 49 CFR 1520.

7. TSA counsel is available to answer questions and provide guidance regarding the identification and treatment of documents that are or may contain SSI for the Court and/or the parties. Questions may be directed to Office of the Chief Counsel, Transportation Security Administration, U.S. Department of Homeland Security, Attn: Virginia Frasure at 571-227-5235.

Sensitive But Unclassified ("SBU") For Official Use Only ("FOUO") Information: DHS Management Directive System, MD No.: 11042.1

8. The designation of For Official Use Only ("FOUO") is used within the Department of Homeland Security ("DHS") to identify unclassified information of a sensitive nature ("Sensitive but Unclassified" or "SBU"), not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal Programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor of successor orders, is not to be considered FOUO. FOUO is not to be considered classified information. See Dept. of Homeland Security Management Directive System, MD Number: 11042.1: "Safeguarding Sensitive But Unclassified (For Official Use Only) Information" ("MD No. 11042.1" attached as Exhibit 2 and incorporated by reference).

9. Access to information classified as SBU or FOUO is limited to those with a "Need-to-know." This determination is made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties. This order permits the sharing through discovery in this civil action of relevant information and materials that are marked SBU or FOUO or may contain SBU or FOUO provided that

Plaintiff had access to such information such information during his employment with Battelle Memorial Institute.

10. The right of access to discovery materials marked as SBU or FOUO or containing SBU or FOUO shall be limited to the Court and its employees, Plaintiff, and counsel for the parties, paralegal and secretarial and clerical personnel in their employ. Court reporters retained by the parties for purposes of recording depositions and who have signed a DHS-approved Non-Disclosure Agreement may also have access to SBU or FOUO.

11. Documents that are marked FOUO or SBU, or though not marked, contain FOUO or SBU shall be treated as confidential and shall not be published or made available to the general public in any form (whether in paper or electronic form), but instead shall be filed under seal.

12. The parties and their representatives are responsible for compliance with the training, physical protection and non-disclosure requirements described in MD No. 11042.1. See Exhibit 2.

13. The designation of information as "sensitive" is left to the discretion of the individual Federal agency. "SBU" is a broad category including information specifically described by statute or regulation, including SSI as well as information not specifically protected by statute or regulation but nonetheless designated as sensitive by the individual agency to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

14. Where FOUO includes SSI information marked as FOUO that meets the standards for designation as SSI, then the SSI guidance for marking, handling, and safeguarding will take precedence.

15. FOUO may also be identified as "Limited Official Use" (LOU") and "Official Use Only" ("OUO") or other similar markings.

16. Information designated as FOUO will be sufficiently marked as "For Official Use Only." Nonetheless, the lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities, where the holder knows the materials to be FOUO.

General Protections Applicable to SSI, SBU, and FOUO Information

17. "Discovery Material" encompassed in this protective order includes, without limitation, deposition testimony, deposition exhibits, interrogatory responses, admissions, affidavits, declarations, documents produced pursuant to compulsory process or voluntarily in lieu of process, and any other documents or information produced or given to one party by another party or by a third party in connection with discovery in this matter. Information taken from Discovery Material that reveals its substance shall also be considered Discovery Material.

18. In addition to any marking required by statute, regulation or DHS guidance, any document containing SSI, SBU or FOUO shall be marked as follows: "Confidential: Subject to SSI, SBU, and FOUO Protective Order in Gary McNair v. Battelle Memorial Institute, dba Pacific Northwest National Laboratory, Civ. Action No. CV-10-5147-RHW." Documents containing SSI, SBU, or FOUO information that inadvertently have not been marked as SSI, SBU, or FOUO still must be safeguarded against unauthorized disclosure.

19. All documents containing or referencing SSI, SBU, or FOUO shall be filed under seal. In order to avoid the inadvertent unsealed filing, the parties shall make all efforts to avoid the unnecessary filing of SSI, SBU, or FOUO with the Court. Material filed under seal will be available only to the persons enumerated in paragraphs two, eight, and nine.

20. Deposition testimony that may contain SSI, SBU, or FOUO information should be so designated by verbal notice or written notice within 10 days of receipt of the transcript. However, testimony containing SSI, SBU, or FOUO information that is not designated, through mistake, nonetheless must be

safeguarded against unauthorized disclosure.

21. All hearings, or portions thereof, in which SSI, SBU, or FOUO information may be disclosed, always shall be closed to the public. If there is a possibility that SSI, SBU, or FOUO information may be disclosed at trial, the courtroom shall be closed to the public.

22. Absent written permission from TSA and/or DHS, the parties may use SSI, SBU, and FOUO information disclosed to them in this Litigation only for the purposes of the Litigation. SSI, SBU, and FOUO information may not be further disseminated, including to a jury, except with written permission from TSA and/or DHS.

23. All documents subject to this Order in the possession of Plaintiff or Plaintiff's counsel shall be returned to Battelle within 60 days of termination of this litigation, including any appellate proceedings, or shall be certified in writing to Battelle to have been properly destroyed by Plaintiff or Plaintiff's counsel.

24. Nothing in this Order shall preclude any disclosure of documents subject to this Order to any Judge, Magistrate, or employee of the Court for purposes of this action.

25. This Order is without prejudice to the rights of any party to make any objection to discovery or use of SSI, SBU, or FOUO or documents that may contain SSI, SBU, or FOUO information permitted by the Federal Rules of Civil Procedure, or any statute, regulation, or other authority.

Personal Identifying Information

26. The parties have an obligation to prevent the unwarranted and unauthorized dissemination of non-party private and confidential information, including, but not limited to, names, addresses, telephone numbers, medical records and information, employment records, and salary information, of current and former employees of Defendant. Accordingly, this information shall be protected from disclosure unless authorized in writing by the subject current or

former employee. If documents containing such material are filed, the personal identifying information shall be redacted from the document filed with the Court.

Federal Rule of Evidence 502 Non-Waiver

27. Pursuant to Federal Rule of Evidence 502 and Federal Rule of Civil Procedure 26(b)(5) the inadvertent and/or accidental disclosure of communication, documents, or information covered by the attorney-client privilege or work product protection shall not result in a waiver of said privilege or protection.

Issues or Disputes Regarding this Protective Order

IT IS SO ORDERED. The District Court Executive is directed to enter this Order and forward copies to counsel.

DATED this 14th day of March, 2011.

ROBERT H. WHALEY
United States District Judge

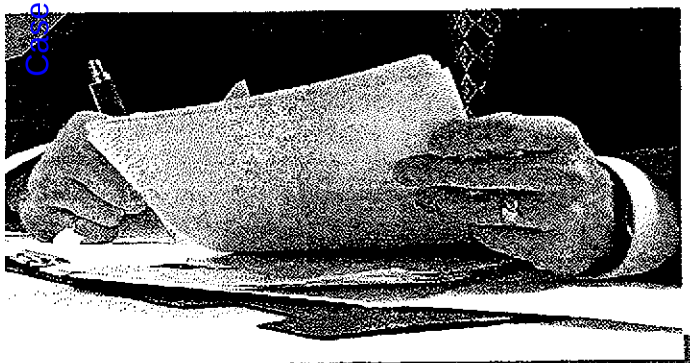
Q:\CIVIL\2010\McNair\protective order.wpd

EXHIBIT 1

Recognizing SSI

SSI is information about transportation security activities. The following information constitutes SSI (as delineated in 49 CFR part 1520):

1. Security programs and contingency plans
2. Security directives
3. Information circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspections or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator



The SSI Office

TSA's Sensitive Security Information (SSI) Office:

- ✓ Develops SSI guidance, policies, and procedures to help others appropriately recognize and handle SSI.
- ✓ Analyzes and reviews records for SSI content.
- ✓ Trains TSA employees, clients, and stakeholders in identifying, handling, marking, sharing, storing, transmitting, and destroying SSI.
- ✓ Coordinates with stakeholders, other governmental agencies, and Congress on SSI-related issues.
- ✓ Provides guidance on and updates to the SSI regulation and other regulations relating to SSI.

www.tsa.gov

For more information, contact us:
The SSI Office
Phone: (571) 227-3513
Fax: (571) 227-2945
SSI@dhs.gov

Sensitive Security Information

✓SSI Quick Reference Guide

Transportation Security Administration

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be detrimental to transportation security.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI.

Marking SSI

Even when only a small portion of a document contains SSI, every page of the document must be marked with the SSI header and footer shown below.

Sensitive Security Information

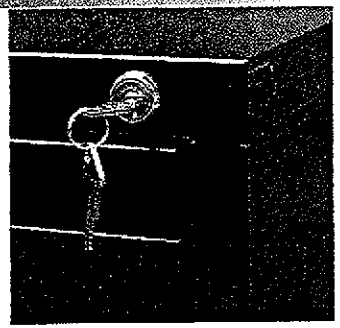
[TEXT]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Handling SSI

- ✓ **Do** make sure all SSI is properly marked.
- ✓ **Do** protect SSI according to the SSI regulation and report any unauthorized disclosures to your SSI Coordinator.
- ✓ **Do** lock up all notes, draft documents, electronic media, and other material containing SSI.
- ✓ **Do** turn off or lock your computer whenever you leave your desk to ensure that no SSI is compromised.
- ✓ **Do** password-protect SSI as an attachment to an email. Do not include the password in the body of the email with the attachment.
- ✓ **Do** personally hand deliver SSI to the intended recipient—never leave SSI unattended in the recipient's work space.
- ✓ **Do** destroy all SSI in your possession when no longer needed.
- ✓ **Do** immediately report any suspected SSI security violation, or poor security practices to your SSI Coordinator.
- ✓ **Do** be conscious of your surroundings when discussing SSI. Protect verbal communications with the same heightened awareness that you would apply to SSI on paper or email.
- ✓ **Do** use encrypted portable devices or password-protect SSI on electronic media.
- ✓ **Do** mail SSI through the U.S. Postal Service, or use other delivery services such as FedEx or UPS. Always wrap SSI in an unmarked opaque envelope, package, or carton.

www.tsa.gov



- ✓ **Don't** leave SSI unattended. Leave it in a locked drawer or locked file cabinet.
- ✓ **Don't** post SSI on any Internet or Intranet web site without prior approval.
- ✓ **Don't** take SSI home, whether on paper or in electronic format, without permission from your supervisor(s).
- ✓ **Don't** share SSI with individuals who do not have a need to know.
- ✓ **Don't** discuss SSI on cordless or cellular phones unless absolutely necessary because these phones can be easily intercepted.
- ✓ **Don't** put SSI in the body of an email—send it as a password-protected attachment.

Destroying SSI

- ✓ Shred with a cross-cut shredder.
- ✓ Cut manually in less than ½-inch squares.
- ✓ Where available, place SSI in designated and clearly marked SSI bins.

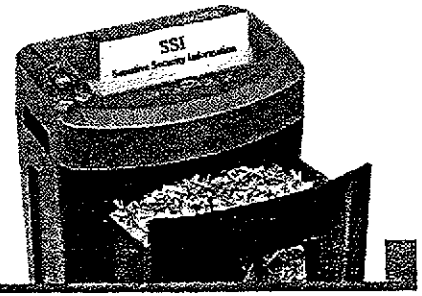


EXHIBIT 2

Department of Homeland Security
Management Directive System
MD Number: 11042.1

SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION

1.6.2005

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

2. Scope

This directive is applicable to all DHS Headquarters, components, organizational elements, detailees, contractors, consultants, and others to whom access to information covered by this directive is granted.

3. Authorities

Homeland Security Act of 2002.

4. Definitions

Access: The ability or opportunity to gain knowledge of information.

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Need-to-know: The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to

perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Organizational Element: As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Sensitive Security Information (SSI): Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

5. Responsibilities

A. The DHS Office of Security will:

1. Be responsible for practical application of all aspects of the program to protect FOUO.

2. Promulgate Department-wide policy guidance.

3. Develop and implement an education and awareness program for the safeguarding of FOUO and other sensitive but unclassified information.

B. Heads of DHS Organizational Elements will:

1. Ensure compliance with the standards for safeguarding FOUO and other sensitive but unclassified information as cited in this directive.

2. Designate an official to serve as a Security Officer or Security Liaison.

C. The organizational element's Security Officer/Security Liaison will:

Be responsible for implementation and oversight of the FOUO information protection program and will serve as liaison between the DHS Office of Security and other organizational security officers.

D. DHS employees, detailees, contractors, consultants and others to whom access is granted will:

1. Be aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.

2. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.

3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

E. Contractors and Consultants shall:

Execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

F. Supervisors and managers will:

1. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.

2. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

6. Policy and Procedures

A. General

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive

order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency.

2. Within the "sensitive but unclassified" arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only; Law Enforcement Sensitive; Official Use Only; Limited Official Use; etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

3. Information shall not be designated as FOUO in order to conceal government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

4. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

B. For Official Use Only

Within DHS, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

(a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.

(b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.

(c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.

(d) Other international and domestic information protected by statute, treaty, regulation or other agreements.

(e) Information that could be sold for profit.

(f) Information that could result in physical risk to personnel.

(g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.

(h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.

(i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

(k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with

sufficient information to clone, counterfeit, or circumvent a process or system.

2. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in this manual. Should the additional guidance be less restrictive than in this directive, the information will be safeguarded in accordance with this directive.

D. Designation Authority

Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited in section 6, paragraph C, as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

F. Marking

1. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., PCII and SSI, etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

(a) Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."

(b) Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.*

(c) Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.*

(d) Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

(f) Individual portion markings on a document that contains no other designation are not required.

(g) Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

G. General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others

and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 6.I) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.

2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.

3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

2. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator.

3. The holder of the information will comply with any access and dissemination restrictions.

4. A security clearance is not required for access to FOUO information.

5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable DHS program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The DHS program office shall then determine if it is appropriate to release the information to the other agency official. (see section 6.F for marking requirements)

7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.

8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.

9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.

2. FOUO information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.

3. IT systems that store FOUO information will be certified and accredited for operation in accordance with federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information.

4. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:

(a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

2. Transmission to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.

3. Electronic Transmission.

(a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

(b) Transmittal via E-Mail

(i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when

transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.

(ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.

(c) DHS Internet/Intranet

(i) FOUO information will not be posted on a DHS or any other internet (public) website.

(ii) FOUO information may be posted on the DHS intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:

(a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

(b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

(c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with IT incident reporting requirements.

2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the DHS Office of Security.

3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day, to the originator and the local Security Official.

4. Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

Dated: 1/6/05

J.M. Loy, ADM
Deputy Secretary of Homeland Security

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

EXHIBIT 3

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	**Protected Critical Infrastructure Information (PCII)**

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	**Sensitive Security Information (SSI)**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	**Other Sensitive but Unclassified (SBU)**

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature: Date:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature: Date:

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.